

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2004-46460

(P2004-46460A)

(43) 公開日 平成16年2月12日(2004.2.12)

(51) Int. Cl.⁷

F I

テーマコード (参考)

G06F 15/00

G06F 15/00 330D

5B017

G06F 12/00

G06F 12/00 537A

5B082

G06F 12/14

G06F 12/14 310K

5B085

H04L 12/66

H04L 12/66 B

5K030

審査請求 未請求 請求項の数 6 O L (全 12 頁)

(21) 出願番号

特願2002-201872 (P2002-201872)

(22) 出願日

平成14年7月10日 (2002.7.10)

(71) 出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(74) 代理人 100088890

弁理士 河原 純一

(72) 発明者 伊藤 秀俊

東京都港区芝五丁目7番1号 日本電気株式会社内

Fターム(参考) 5B017 AA03 AA07 BA05 BA06 BB06

BB10 CA16

5B082 EA11 EA12 GA13

5B085 AA08 AE02 AE06 AE15 AE23

BC02 BG02 BG07 CA02 CA04

5K030 GA15 HA08 HC01 HC13 HD03

KA04 LD19

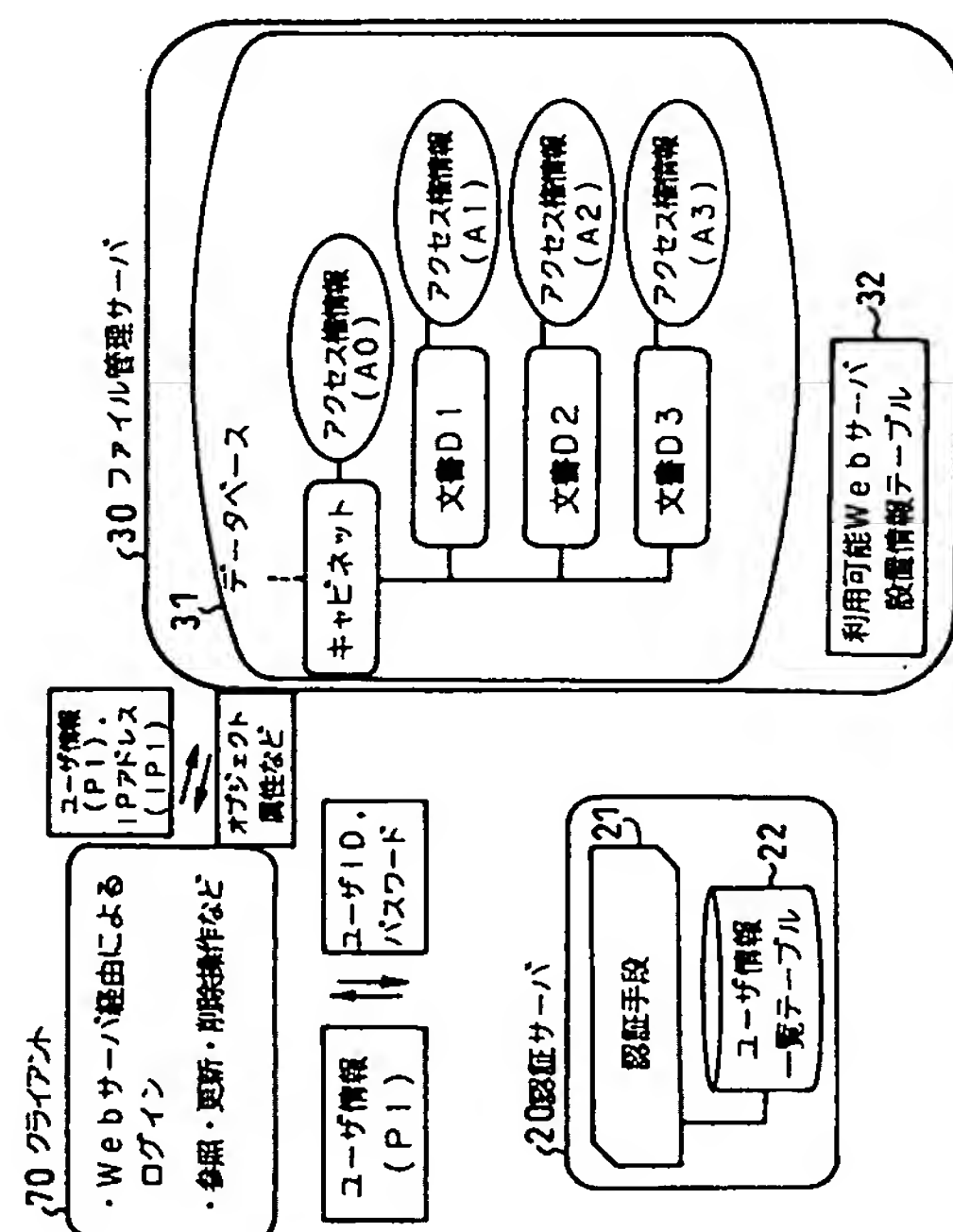
(54) 【発明の名称】 ファイル管理システムにおけるアクセス制御方式

(57) 【要約】

【課題】 同一ユーザによる同一オブジェクトへのアクセスであっても、社内・社外どちらからのアクセスかに応じて、異なるアクセス権を設定可能とする。

【解決手段】 クライアント70は、キャビネット、文書等のオブジェクトへのアクセス時にユーザ情報およびログイン時に経由したWebサーバのIPアドレスをファイル管理サーバ30に渡す。ファイル管理サーバ30は、利用可能Webサーバ設置情報テーブル32に登録されているIPアドレスに対応する設置情報を取得し、ユーザ情報および設置情報をキーとしてオブジェクトのアクセス権情報を検索してユーザのオブジェクトへのアクセス権の有無を判定する。

【選択図】 図1



【特許請求の範囲】

【請求項 1】

Web ベースのファイル管理システムにおいて、
クライアントからファイル管理サーバへのログインの要求時に、クライアントから受け取ったユーザ ID がユーザ情報一覧テーブルに登録されているかどうかをチェックし、ユーザ ID が登録されていたならばクライアントから受け取ったパスワードが前記ユーザ情報一覧テーブルにユーザ ID に対応して登録されているパスワードと一致するかどうかをチェックし、パスワードが一致した場合には前記ユーザ情報一覧テーブルから該当ユーザのユーザ情報を取得してクライアントに返却する認証サーバと、
対象オブジェクトを示すインスタンス ID、前記認証サーバから得られたユーザ情報、およびログイン時に経由した Web サーバの IP アドレスを前記ファイル管理サーバに渡すクライアントと、
オブジェクト、およびオブジェクト毎のアクセス権情報を登録するデータベースと、利用可能 Web サーバ設置情報テーブルとを備え、クライアントからのオブジェクトへのアクセス要求があったときに、前記利用可能 Web サーバ設置情報テーブルから前記 IP アドレスに対応する設置情報を取得し、ユーザ情報および設置情報をキーとして対象オブジェクトのアクセス権情報を検索してユーザの対象オブジェクトへのアクセス権の有無を判定し、ユーザが対象オブジェクトへのアクセス権を有しているときにオブジェクトにアクセスし、アクセス結果を前記クライアントに送信するファイル管理サーバと
を有することを特徴とするファイル管理システムにおけるアクセス制御方式。 10 20

【請求項 2】

前記アクセス権情報が、少なくとも、ユーザを示す要求元と、ログイン時に経由した Web サーバがファイアウォールの内に存在するか外に存在するかを示す設置情報と、ユーザのオブジェクトへのアクセス権の有無とを含むことを特徴とする請求項 1 記載のファイル管理システムにおけるアクセス制御方式。

【請求項 3】

前記利用可能 Web サーバ設置情報テーブルが、Web サーバの IP アドレスと、Web サーバがファイアウォールの内に存在するか外に存在するかを示す設置情報とを含むことを特徴とする請求項 1 記載のファイル管理システムにおけるアクセス制御方式。

【請求項 4】

クライアントがファイル管理サーバへのログイン時に認証サーバから認証結果としてユーザ情報を取得するとともに経由した Web サーバの IP アドレスを取得する工程と、
クライアントがオブジェクトへのアクセス要求時に前記ユーザ情報および前記 IP アドレスをファイル管理サーバに渡す工程と、
ファイル管理サーバが利用可能 Web サーバ設置情報テーブルに前記 IP アドレスが登録されているかどうかを判定する工程と、
前記 IP アドレスが登録されているときにファイル管理サーバが前記利用可能 Web サーバ設置情報テーブルから前記 IP アドレスに対応する設置情報を取得する工程と、
ファイル管理サーバがユーザ情報および設置情報をキーとして対象オブジェクトのアクセス権情報を検索しユーザのオブジェクトへのアクセス権の有無を判定する工程と、
ユーザがオブジェクトへのアクセス権を有しているときにファイル管理サーバが対象オブジェクトにアクセスしてアクセス結果をクライアントに送信する工程と、
クライアントがファイル管理サーバからオブジェクトのアクセス結果を受信する工程とを含むことを特徴とするファイル管理システムにおけるアクセス制御方法。 30 40 50

【請求項 5】

コンピュータに、ファイル管理サーバへのログイン時に認証サーバのから認証結果としてユーザ情報を取得するとともに経由した Web サーバの IP アドレスを取得する工程と、オブジェクトへのアクセス要求時に前記ユーザ情報および前記 IP アドレスをファイル管理サーバに渡す工程と、ファイル管理サーバからオブジェクトのアクセス結果を受信する工程とを実行させるためのプログラム。

【請求項 6】

コンピュータに、利用可能 Web サーバ 設置情報 テーブルを参照して IP アドレスが登録されているかどうかを判定する工程と、前記 IP アドレスが登録されているときに前記利用可能 Web サーバ 設置情報 テーブルから前記 IP アドレスに対応する設置情報を取得する工程と、ユーザ情報および設置情報をキーとしてアクセス権情報を検索しユーザのオブジェクトへのアクセス権の有無を判定する工程と、ユーザがオブジェクトへのアクセス権を有しているときにオブジェクトにアクセスし、アクセス結果をクライアントに送信する工程とを実行させるためのプログラム。

【発明の詳細な説明】

【0001】

10

【発明の属する技術分野】

本発明はファイル管理システムにおけるアクセス制御方式に関し、特に Web ベースのファイル管理システムにおける社内・社外ログイン時のアクセス制御方式に関する。

【0002】

【従来の技術】

今日では、インターネット等の技術進歩により社内・社外を問わず、また会社間の垣根を越えた共通のワークスペース（コーポレートウェアなど）が提供されており、そのニーズも拡大している。このように、ファイル管理システムなどにおけるシームレス化が進む一方で、セキュリティ面での強化がますます要求されている。

【0003】

20

ところで、従来のファイル管理システムにおけるアクセス制御方法としては、端末グループによってアクセス権を異ならしめたり（特開平 02-282842 参照）、時間帯に応じてアクセスの妥当性を変化させたり（特開平 02-285439 参照）、プレゼンテーションの内容を使用者によって抑止させたり（特開平 03-154969 参照）する各種の方法が知られていた。

【0004】

【発明が解決しようとする課題】

しかし、従来の技術では、ユーザが、社内からキャビネット、フォルダ、文書（ドキュメント）などのオブジェクトにアクセスする場合でも、社外からオブジェクトにアクセスする場合でも、同じセキュリティのレベルであり、特に社外からオブジェクトにアクセスする場合には社内からオブジェクトにアクセスする場合に比べてセキュリティ面での強化を行いたいという要請があっても行えないという問題点があった。その理由は、ファイル管理サーバでは、キャビネット、フォルダ、文書などのオブジェクト単位で権利認証（Authentication）に利用されるアクセス権を設定可能であったが、同一ユーザが社内から同一オブジェクトにアクセスした場合でも、社外から同一オブジェクトにアクセスした場合でも、オブジェクトに設定されるアクセス権情報が同じであったからである。

30

【0005】

本発明の目的は、Web ベースのファイル管理システムにおいて、同一ユーザからの同一オブジェクトへのアクセスについて、社内からのアクセスであるか社外からのアクセスであるかに応じて、異なるアクセス権を設定可能なファイル管理システムにおけるアクセス制御方式を提供することにある。

40

【0006】

また、本発明の他の目的は、Web ベースのファイル管理システムにおいて、同一ユーザによる同一オブジェクトへのアクセスであっても、社内からのアクセスであるか社外からのアクセスであるかに応じて、権利認証を異ならしめるようにしたファイル管理システムにおけるアクセス制御方法を提供することにある。

【0007】

【課題を解決するための手段】

本発明のファイル管理システムにおけるアクセス制御方式は、Web ベースのファイル管理システムにおいて、クライアントからファイル管理サーバへのログインの要求時に、ク

50

クライアントから受け取ったユーザIDがユーザ情報一覧テーブルに登録されているかどうかをチェックし、ユーザIDが登録されていたならばクライアントから受け取ったパスワードが前記ユーザ情報一覧テーブルにユーザIDに対応して登録されているパスワードと一致するかどうかをチェックし、パスワードが一致した場合には前記ユーザ情報一覧テーブルから該当ユーザのユーザ情報を取得してクライアントに返却する認証サーバと、対象オブジェクトを示すインスタンスID、前記認証サーバから得られたユーザ情報、およびログイン時に経由したWebサーバのIPアドレスを前記ファイル管理サーバに渡すクライアントと、オブジェクト、およびオブジェクト毎のアクセス権情報を登録するデータベースと、利用可能Webサーバ設置情報テーブルとを備え、クライアントからのオブジェクトへのアクセス要求があったときに、前記利用可能Webサーバ設置情報テーブルから前記IPアドレスに対応する設置情報を取得し、ユーザ情報および設置情報をキーとして対象オブジェクトのアクセス権情報を検索してユーザの対象オブジェクトへのアクセス権の有無を判定し、ユーザが対象オブジェクトへのアクセス権を有しているときにオブジェクトにアクセスし、アクセス結果を前記クライアントに送信するファイル管理サーバとを有することを特徴とする。

10

【0008】

また、本発明のファイル管理システムにおけるアクセス制御方式は、前記アクセス権情報が、少なくとも、ユーザを示す要求元と、ログイン時に経由したWebサーバがファイアウォールの内に存在するか外に存在するかを示す設置情報と、ユーザのオブジェクトへのアクセス権の有無とを含むことを特徴とする。

20

【0009】

さらに、本発明のファイル管理システムにおけるアクセス制御方式は、前記利用可能Webサーバ設置情報テーブルが、WebサーバのIPアドレスと、Webサーバがファイアウォールの内に存在するか外に存在するかを示す設置情報とを含むことを特徴とする。

【0010】

一方、本発明のファイル管理システムにおけるアクセス制御方法は、クライアントがファイル管理サーバへのログイン時に認証サーバから認証結果としてユーザ情報を取得するとともに経由したWebサーバのIPアドレスを取得する工程と、クライアントがオブジェクトへのアクセス要求時に前記ユーザ情報および前記IPアドレスをファイル管理サーバに渡す工程と、ファイル管理サーバが利用可能Webサーバ設置情報テーブルに前記IPアドレスが登録されているかどうかを判定する工程と、前記IPアドレスが登録されているときにファイル管理サーバが前記利用可能Webサーバ設置情報テーブルから前記IPアドレスに対応する設置情報を取得する工程と、ファイル管理サーバがユーザ情報および設置情報をキーとして対象オブジェクトのアクセス権情報を検索しユーザのオブジェクトへのアクセス権の有無を判定する工程と、ユーザがオブジェクトへのアクセス権を有しているときにファイル管理サーバが対象オブジェクトにアクセスしてアクセス結果をクライアントに送信する工程と、クライアントがファイル管理サーバからオブジェクトのアクセス結果を受信する工程とを含むことを特徴とする。

30

【0011】

他方、本発明のプログラムは、コンピュータに、ファイル管理サーバへのログイン時に認証サーバのから認証結果としてユーザ情報を取得するとともに経由したWebサーバのIPアドレスを取得する工程と、オブジェクトへのアクセス要求時に前記ユーザ情報および前記IPアドレスをファイル管理サーバに渡す工程と、ファイル管理サーバからオブジェクトのアクセス結果を受信する工程とを実行させることを特徴とする。

40

【0012】

また、本発明のプログラムは、コンピュータに、利用可能Webサーバ設置情報テーブルを参照してIPアドレスが登録されているかどうかを判定する工程と、前記IPアドレスが登録されているときに前記利用可能Webサーバ設置情報テーブルから前記IPアドレスに対応する設置情報を取得する工程と、ユーザ情報および設置情報をキーとしてアクセス権情報を検索しユーザのオブジェクトへのアクセス権の有無を判定する工程と、ユーザ

50

がオブジェクトへのアクセス権を有しているときにオブジェクトにアクセスし、アクセス結果をクライアントに送信する工程とを実行させることを特徴とする。

【0013】

本発明は、ファイル管理サーバへのログイン時に経由する社内Webサーバまたは社外Webサーバの設置情報（ファイアウォール内・外の情報）を、ファイル管理サーバで行う権利認証の中で利用することを特徴とするものである。ユーザがクライアントから社内Webサーバを経由してファイル管理サーバにログインした場合にはアクセス対象のオブジェクト（以下、対象オブジェクトという）にアクセスすることができる一方、クライアントから社外Webサーバを経由してファイル管理サーバにログインした場合には対象オブジェクトにアクセスすることができないようにすることができる。このため、Webサーバの設置情報を、そのままユーザからのファイル管理サーバへのアクセス権情報の一部として利用する。

【0014】

【発明の実施の形態】

以下、本発明の実施の形態について図面を参照して詳細に説明する。

【0015】

〔第1の実施の形態〕

図2は、本発明の第1の実施の形態に係るアクセス制御方式が適用されるファイル管理システムのシステム構成図である。このファイル管理システムは、ローカルエリアネットワーク（LAN）等なる社内ネットワーク10と、社内ネットワーク10に接続された認証サーバ20と、社内ネットワーク10に接続されたファイル管理サーバ30と、社内ネットワーク10に接続されたWebサーバ（以下、社内Webサーバという）40と、社内ネットワーク10に接続されたファイアウォール50と、ファイアウォール50およびインターネット等の外部回線に接続されたWebサーバ（以下、社外Webサーバという）60と、社内Webサーバ40または社外Webサーバ60を経由してファイル管理サーバ30にログインする複数のクライアント70とから構成されている。

【0016】

図1を参照すると、認証サーバ20は、認証手段21と、ユーザ情報一覧テーブル22とを含んで構成されている。

【0017】

図3は、認証サーバ20で管理しているユーザ情報一覧テーブル22のデータ構造図を示す。ユーザ情報一覧テーブル22には、ファイル管理サーバ30にログインを許可されているユーザのユーザID（Identification）、ユーザ名、パスワード、所属部署ID、所属部署名などからなるユーザ情報が登録されて一括管理されている。

【0018】

図1を参照すると、ファイル管理サーバ30は、データベース31と、利用可能Webサーバ設置情報テーブル32とを含んで構成されている。

【0019】

データベース31は、キャビネット、文書等のオブジェクトをツリー状に階層的に保持しており、各オブジェクトは、アクセス権情報（A*）（*はワイルドカードであることを表す）を属性として持っている。各オブジェクト（インスタンス）は、データベース31上で登録時に自動生成される一意なインスタンスIDを持っており、オブジェクトを指定するにはインスタンスIDが用いられる。インスタンスIDは、クライアント70からファイル管理サーバ30に、ユーザ情報（P1）、および社内Webサーバ40または社外Webサーバ60のIPアドレス（IP1）とともに渡される。図1の例では、データベース31は、“キャビネット”およびその配下に“文書D1”、“文書D2”、“文書D3”を含む。また、“文書D1”には、アクセス権情報A1が属性として登録されている（他のオブジェクトも同様）。

【0020】

図4を参照すると、アクセス権情報（A*）は、オブジェクト毎に1つの表で管理されて

10

20

30

40

50

おり、ユーザ情報（P*）を用いた条件式の組み合わせ（AND条件、OR条件など）の形で設定が可能である。アクセス権情報（A*）は、要求元と、役職範囲と、設置情報と、アクセス権（参照権、更新権および削除権）の有無とを含む。要求元は、ユーザ、所属部署等を表す文字列である。役職範囲には、例えば、名前、所属部署名、勤務地、役職等が格納される。設置情報は、社内Webサーバ40または社外Webサーバ60のどちらを経由してファイル管理サーバ30にログインしたかという条件（0で社内Webサーバ40、1で社外Webサーバ60）である。アクセス権（参照権、更新権および削除権）の有無は、理解しやすいように○や×として表記しているが、データベース31上では数値として管理されている。

【0021】

ファイル管理サーバ30では、キャビネット、文書などの各オブジェクトに対する設定可能なアクセス権の種類として、参照権、更新権、削除権等が定義されている。例えば、クライアント70からあるオブジェクトの参照が要求された場合、ファイル管理サーバ30は、要求元のユーザが対象オブジェクトに対して参照権を有するかどうかを権利認証する。

【0022】

ファイル管理サーバ30は、社内Webサーバ40または社外Webサーバ60の設置情報をアクセス権情報の1つのカテゴリとして組み込むことにより、ユーザの対象オブジェクトへのアクセス時の権利認証の際には、経由した社内Webサーバ40または社外Webサーバ60の設置情報と適合するアクセス権情報（A*）のみが権利認証の対象となる（に切り分けられて判定される）。

【0023】

図5は、利用可能Webサーバ設置情報テーブル32のデータ構造を示す図である。利用可能Webサーバ設置情報テーブル32は、IPアドレスと、Webサーバがファイアウォール50内外のどちらに設置されているかの設置情報（0でファイアウォール50内、1でファイアウォール50外）とがレコードとして、ファイル管理サーバ30にログインする上で経由可能な社内Webサーバ40および社外Webサーバ60の数分だけ登録されている。ファイル管理サーバ30は、ユーザ情報およびIPアドレスと、利用可能Webサーバ設置情報テーブル32とに基づいてユーザのオブジェクトに対する権利認証を行う。

【0024】

ファイル管理サーバ30は、クライアント70から渡される経由WebサーバのIPアドレス（IP1）のみでは、ファイアウォール50内外のどちらに設置されているWebサーバを経由してログインしたかは判断できないので、ファイル管理サーバ30の利用可能Webサーバ設置情報テーブル32に設置情報をあらかじめ登録しておく。

【0025】

図6を参照すると、認証サーバ20におけるユーザ認証（Authentication）処理は、ユーザID登録判定ステップS101と、パスワード正否判定ステップS102と、ユーザ情報返却ステップS103とからなる。

【0026】

図7を参照すると、ファイル管理サーバ30における権利認証（Authorization）処理は、IPアドレス登録判定ステップS201と、設置情報取得ステップS202と、オブジェクト存在判定ステップS203と、ユーザアクセス権有無判定ステップS204と、オブジェクト返却ステップS205とからなる。

【0027】

次に、このように構成された第1の実施の形態に係るファイル管理システムにおけるアクセス制御方式の動作について説明する。

【0028】

（1） 認証サーバ20によるユーザ認証（Authentication）について

【0029】

10

20

30

40

50

ユーザは、ファイル管理サーバ30のオブジェクトにアクセスする前に、クライアント70から社内Webサーバ40または社外Webサーバ60を経由してファイル管理サーバ30にログインする必要がある。ユーザは、通常、社内ネットワーク10に接続されているクライアント70からファイアウォール50内に設置されている社内Webサーバ40を経由してファイル管理サーバ30にログインする。しかし、出張先や家庭などのクライアント70からファイル管理サーバ30にログインする場合には、ユーザは、ファイアウォール50外に設置されている社外Webサーバ60を経由した場合に限りファイル管理サーバ30にログイン可能である。ただし、ユーザが社内から社外Webサーバ60を経由してオブジェクトにアクセスすることは、ファイアウォール50で制限されていない限りは可能である。

10

【0030】

ユーザがクライアント70から社内Webサーバ40または社外Webサーバ60を経由してファイル管理サーバ30にログインする際に、認証サーバ20によるユーザ認証が行われる。

【0031】

詳しくは、ユーザは、クライアント70のログイン画面からユーザIDおよびパスワードを入力し、ファイル管理サーバ30へのログインを要求する。この際、クライアント70と認証サーバ20との通信が行われ、認証サーバ20によるユーザ認証が行われる。なお、クライアント70とファイル管理サーバ30との通信が行われるのは、クライアント70で、属性一覧の取得、更新画面での更新確定、キャビネット、フォルダなどの配下一覧の取得、対象の削除などの操作ボタンが押下された時点である。

20

【0032】

認証サーバ20は、まず、クライアント70から受け取ったユーザIDがユーザ情報一覧テーブル22に登録されているかどうかをチェックする（ステップS101）。ユーザIDが登録されていないければ、認証サーバ20は、エラーをクライアント70に返却する。

【0033】

ユーザIDが登録されていたならば、認証サーバ20は、クライアント70から受け取ったパスワードがユーザ情報一覧テーブル22にユーザIDと対応して登録されているパスワードと一致するかどうかをチェックする（ステップS102）。パスワードが一致しなかった場合、認証サーバ20は、エラーをクライアント70に返却する。

30

【0034】

パスワードが一致した場合には、認証サーバ20は、ユーザ情報一覧テーブル22から該当ユーザのユーザ情報（P1）を取得してクライアント70に返却し（ステップS103）、処理を終了する。

【0035】

ファイル管理サーバ30へのログインと同時にキャビネット一覧テーブル（図示せず）の取得が行われ、クライアント70の画面には、通常、ユーザ固有のキャビネット一覧テーブルが表示される。キャビネット一覧テーブルに表示されているオブジェクトは、ログインしたユーザがアクセス権を有しているもののみであり、キャビネット一覧テーブルに表示されているのは各オブジェクトの一部の属性のみである。

40

【0036】

（2） ファイル管理サーバ30における権利認証（Authorization）

【0037】

クライアント70の画面にユーザ固有のキャビネット一覧テーブル（図示せず）が表示された後、ユーザがクライアント70からオブジェクトへのアクセスを要求した場合、ファイル管理サーバ30は、要求元のユーザがアクセス対象のオブジェクト（以下、対象オブジェクトという）のアクセス権を有するかどうかを権利認証する。

【0038】

まず、クライアント70は、対象オブジェクトを示すインスタンスIDを、認証サーバ20から得られたユーザ情報、および社内Webサーバ40または社外Webサーバ60の

50

IPアドレス（IP1）とともに、ファイル管理サーバ30に渡す。

【0039】

ファイル管理サーバ30は、ユーザ認証で取得されたユーザ情報（P1）と、経由した社内Webサーバ40または社外Webサーバ60のIPアドレス（IP1）とを元に、対象オブジェクトに対するユーザの権利認証を行う。

【0040】

ここで、ユーザH（ユーザ情報P1）が”文書D1”の参照を要求する場合を考える（図5参照）。”文書D1”には、要求元であるユーザHに関して、図5に示すようなアクセス権情報（A1）が属性として設定されているものとする。

【0041】

クライアント70で”キャビネット”配下のオブジェクト一覧を表示中（”文書D1”は一部の属性のみしか表示されていない）に、ユーザHが”文書D1”の参照要求を行うと（参照ボタンを押下すると）、クライアント70は、ユーザ情報（P1）、および経由Webサーバ（社内Webサーバ40または社外Webサーバ60）のIPアドレス（IP1）をファイル管理サーバ30に渡す。

【0042】

ファイル管理サーバ30は、まず、クライアント70から渡された経由WebサーバのIPアドレス（IP1）が、利用可能Webサーバ設置情報テーブル32に登録されているかどうかを判定する（ステップS201）。

【0043】

IPアドレス（IP1）が利用可能Webサーバ設置情報テーブル32に登録されていれば、ファイル管理サーバ30は、経由WebサーバのIPアドレスに対応する設置情報（0でファイアウォール50内、1でファイアウォール50外）を取得する（ステップS202）。

【0044】

次に、ファイル管理サーバ30は、インスタンスIDにより”文書D1”がデータベース31上に存在するか否かをチェックする（ステップS203）。ファイル管理サーバ30は、データベース31上に存在するオブジェクトに対応する一覧テーブルを一括管理しており、インスタンスIDと一覧テーブルのデータとの比較処理を行う。

【0045】

”文書D1”がデータベース31上に存在する場合、ファイル管理サーバ30は、要求元のユーザHが”文書D1”の参照権を有しているかどうかの権利認証を行う（ステップS204）。詳しくは、ファイル管理サーバ30は、まず、”文書D1”のアクセス権情報（A1）を取得する。このとき、経由WebサーバのIPアドレスが利用可能Webサーバ設置情報テーブル32に登録されており、当該IPアドレスに対応する設置情報が0と判定されたとすれば、ファイル管理サーバ30は、「ユーザHに対して参照および更新が可能」という条件のみが権利認証の対象となる。したがって、この場合、ファイル管理サーバ30は、ユーザHが”文書D1”の参照権および更新権を有することを判定する。

【0046】

次に、ファイル管理サーバ30は、データベース31から文書D1およびその属性を取得し、クライアント70へ返却する（ステップS205）。

【0047】

クライアント70は、ファイル管理サーバ30から文書D1およびその属性を受信すると、これらを参照することができる。

【0048】

なお、上記動作の説明では、アクセスが参照である場合を例にとって説明したが、アクセスが更新および削除の場合であっても、ほぼ同様の動作となることはいうまでもない。

【0049】

また、オブジェクトを文書とした場合を例にとって説明したが、オブジェクトへのアクセス制御を、文書単位のみではなく、フォルダ単位やキャビネット単位でも行うことが可能

10

20

30

40

50

であることをいうまでもない。

【0050】

このように、第1の実施の形態によれば、ファイル管理サーバ30へのログイン時に経由したWebサーバが社内是否存在するか社外是否存在するかを加味して権利認証を行う仕組みを設けることにより、同一ユーザからの同一オブジェクトへのアクセスについても、社内からアクセスしたか社外からアクセスしたかに応じて権利認証を異ならしめることができる。例えば、同一ユーザからの同一オブジェクトへのアクセスに関して、参照は社内からでも社外からでも可能とする一方、更新は社内からでなければ許可しないようにすることが可能となる。

【0051】

〔第2の実施の形態〕

図8は、本発明の第2の実施の形態に係るファイル管理システムにおけるアクセス制御方式の構成を示すブロック図である。本実施の形態に係るファイル管理システムにおけるアクセス制御方式は、図1に示した第1の実施の形態に係るファイル管理システムにおけるアクセス制御方式に対して、認証サーバ20に認証サーバプログラム200を備え、ファイル管理サーバ30にファイル管理サーバプログラム300を備えている点だけが異なっている。

【0052】

認証サーバプログラム200は、コンピュータである認証サーバ20に読み込まれ、当該認証サーバ20の動作を認証手段21およびユーザ情報一覧テーブル22として制御する。認証サーバプログラム200の制御による認証サーバ20の動作は、第1の実施の形態における認証サーバ20の動作と全く同様になるので、その詳しい説明を割愛する。

【0053】

また、ファイル管理サーバプログラム300は、コンピュータであるファイル管理サーバ30に読み込まれ、当該ファイル管理サーバ30の動作をデータベース31および利用可能Webサーバ設置情報テーブル32として制御する。ファイル管理サーバプログラム300の制御によるファイル管理サーバ30の動作は、第1の実施の形態におけるファイル管理サーバ30の動作と全く同様になるので、その詳しい説明を割愛する。

【0054】

〔発明の効果〕

第1の効果は、アクセス権として設定可能な条件の幅を広げることにより、多様化するユーザの利用局面に対応したアクセス制御機能が提供できることである。その理由は、ファイル管理サーバへのログイン時に経由したWebサーバが社内是否存在するか社外是否存在するかを加味して権利認証を行う仕組みを設けるようにしたからである。

【0055】

第2の効果は、それに伴いセキュリティ面での強化も図ることが可能であることである。その理由は、例えば、同一ユーザからの同一オブジェクトへのアクセスに関して、参照は社内からでも社外からでも可能とする一方、更新は社内からでなければ許可しないようにすることが可能であるからである。

〔図面の簡単な説明〕

【図1】本発明の第1の実施の形態に係るファイル管理システムにおけるアクセス制御方式の構成を示すブロック図である。

【図2】第1の実施の形態に係るアクセス制御方式が適用されるファイル管理システムのシステム構成図である。

【図3】図1中の認証サーバで管理されるユーザ情報一覧テーブルのデータ構造図である。

【図4】図1中のデータベースで管理されるアクセス権情報のデータ構造図である。

【図5】図1中の利用可能Webサーバ設置情報テーブルのデータ構造図である。

【図6】図1中の認証サーバにおけるユーザ認証処理を示すフローチャートである。

【図7】図1中のファイル管理サーバにおける権利認証処理を示すフローチャートである

10

20

30

40

50

。【図 8】本発明の第 2 の実施の形態に係るファイル管理システムにおけるアクセス制御方式の構成を示すブロック図である。

【符号の説明】

- 10

社内ネットワーク
- 20

認証サーバ
- 21

認証手段
- 22

ユーザ情報一覧テーブル
- 30

ファイル管理サーバ
- 31

データベース
- 32

利用可能Webサーバ設置情報テーブル
- 40

社内Webサーバ
- 50

ファイアウォール
- 60

社外Webサーバ
- 70

クライアント
- 200

認証サーバプログラム
- 300

ファイル管理サーバプログラム
- S101

ユーザID登録判定ステップ
- S102

パスワード正否判定ステップ
- S103

ユーザ情報返却ステップ
- S201

IPアドレス登録判定ステップ
- S202

設置情報取得ステップ
- S203

オブジェクト存在判定ステップ
- S204

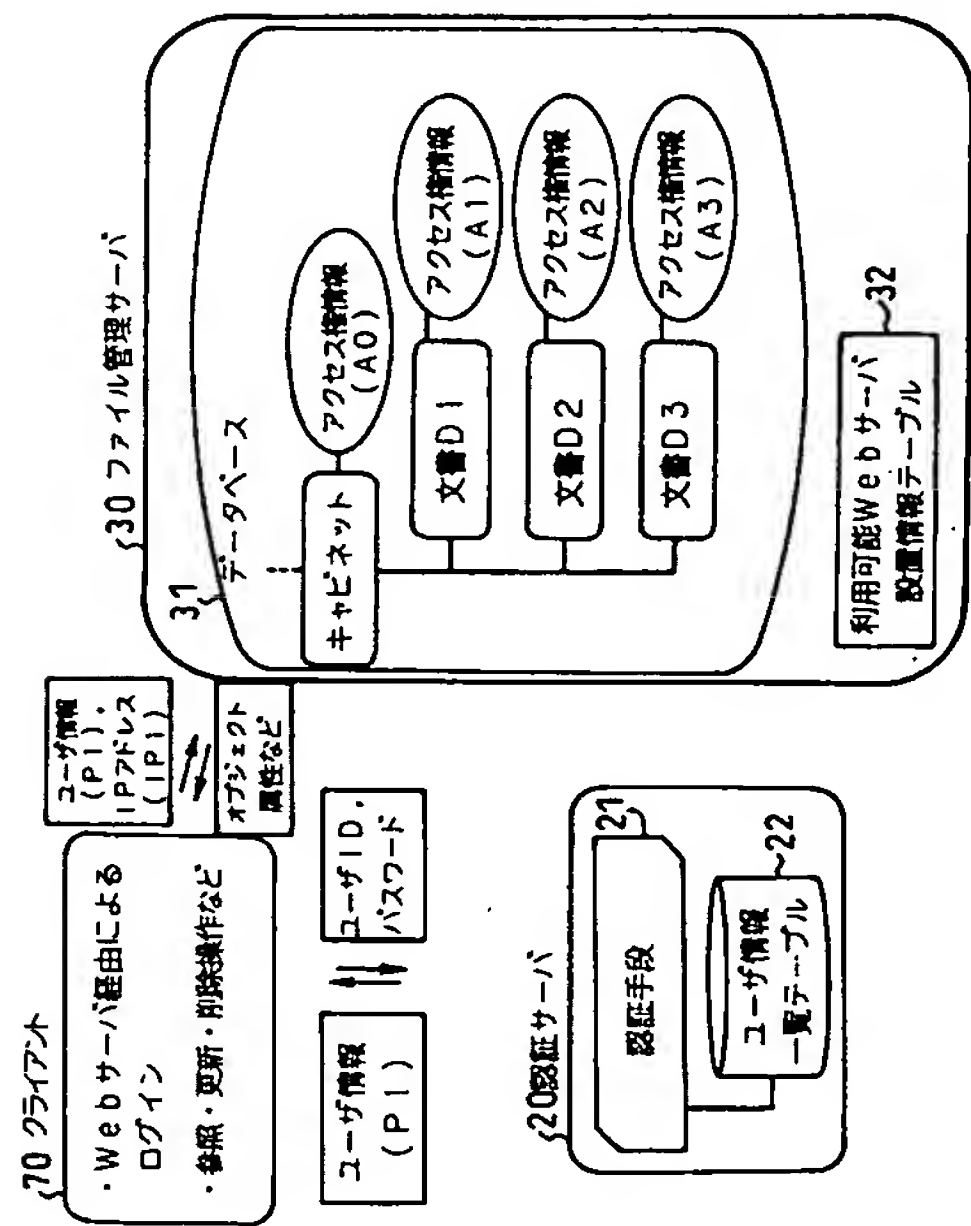
ユーザアクセス権有無判定ステップ
- S205

オブジェクト返却ステップ

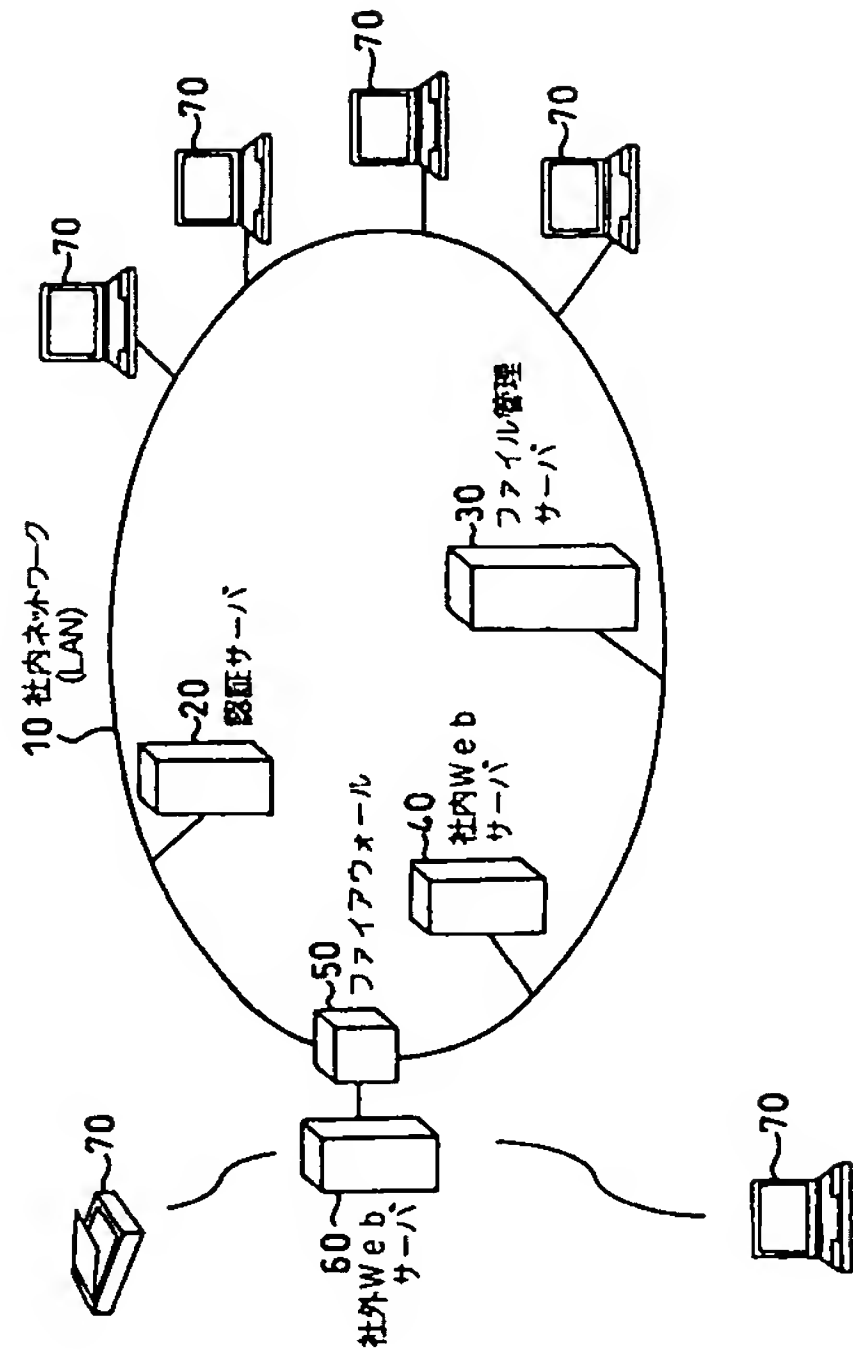
10

20

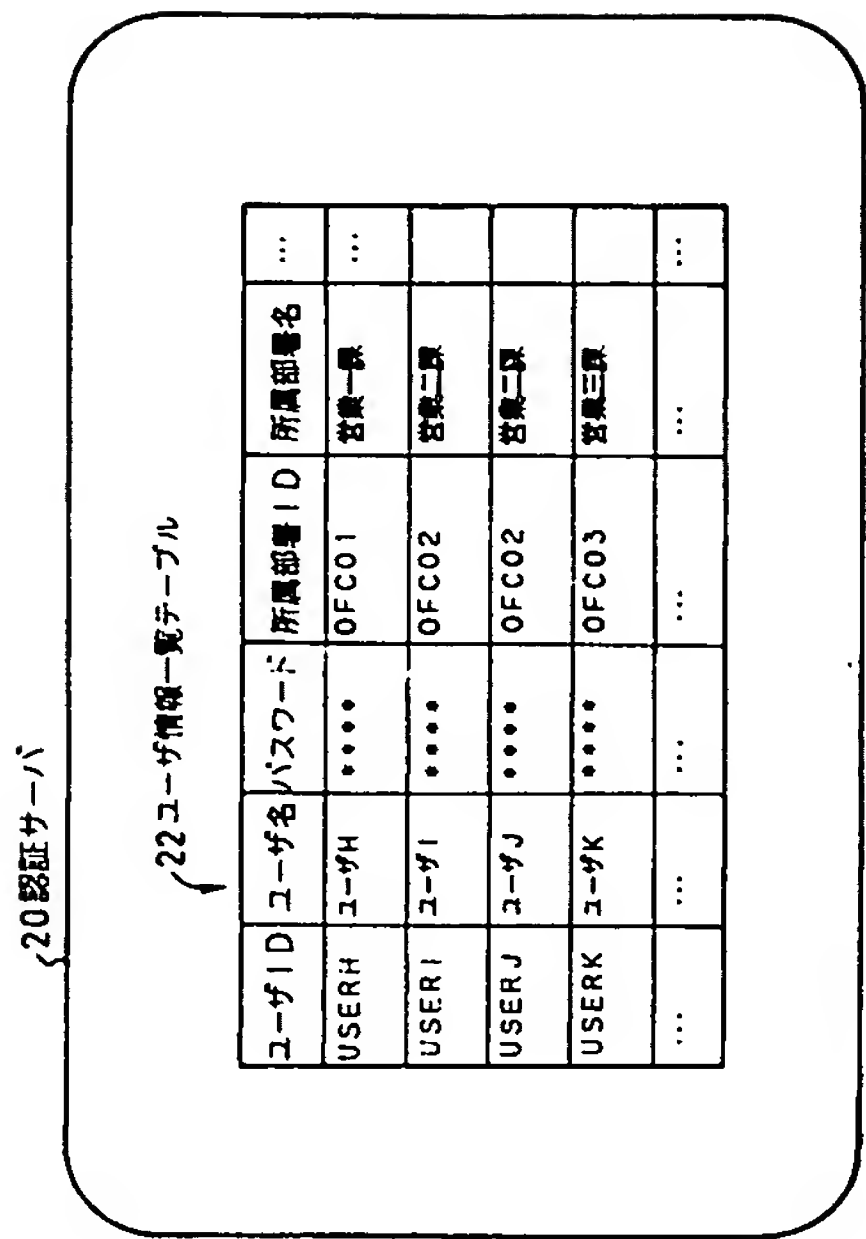
【図 1】



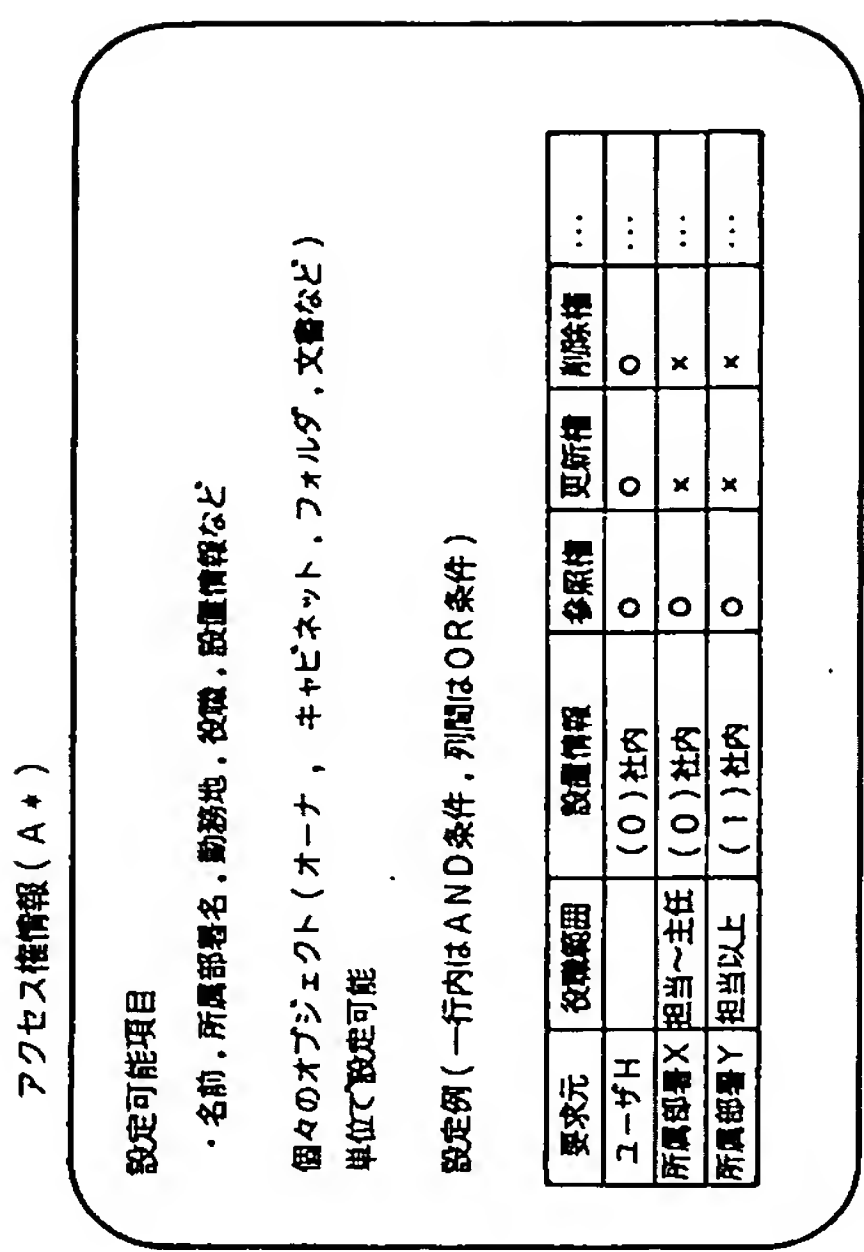
【図 2】



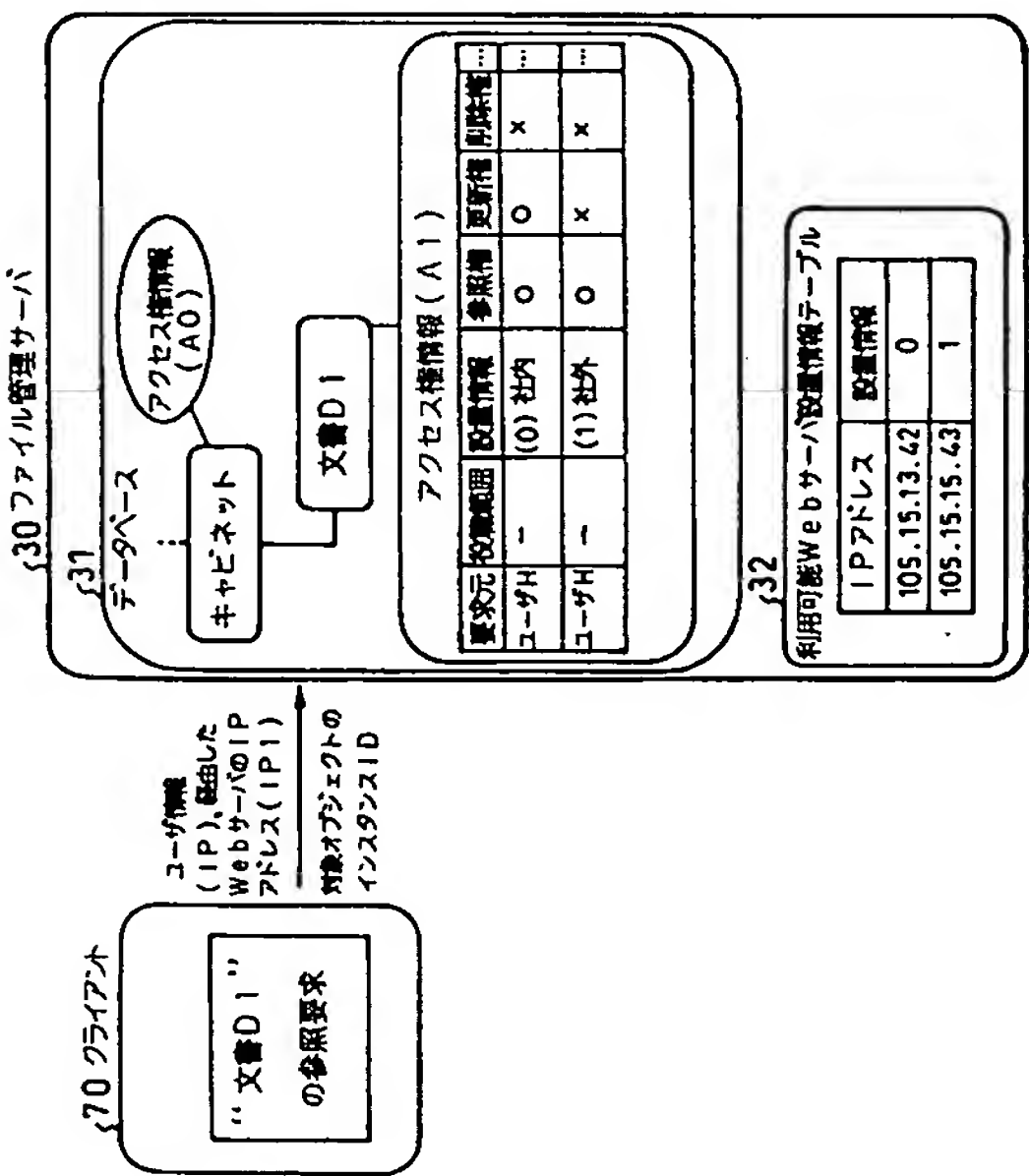
【図 3】



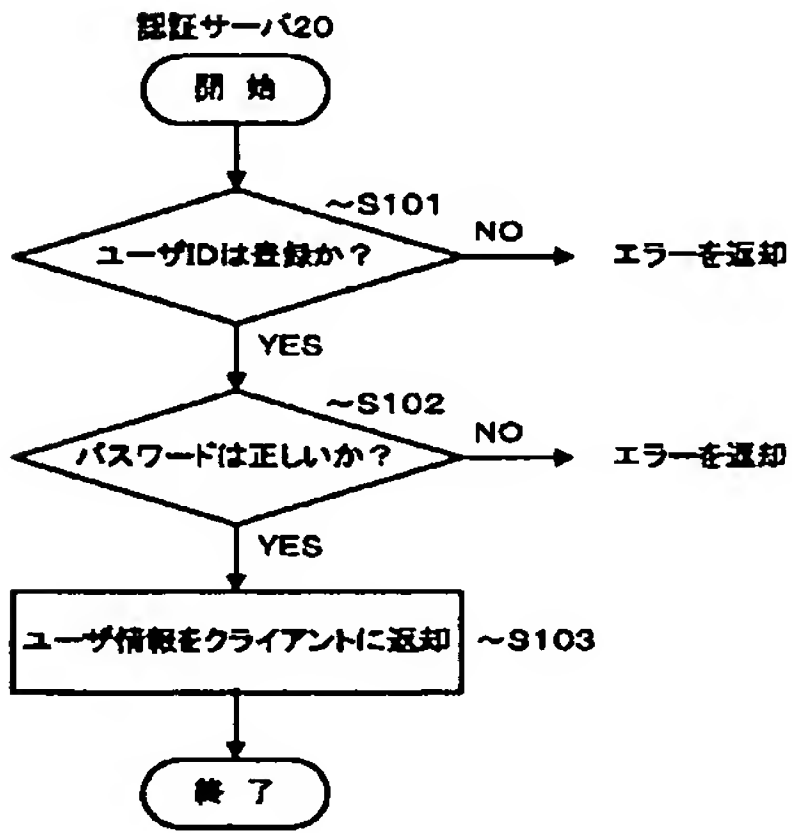
【図 4】



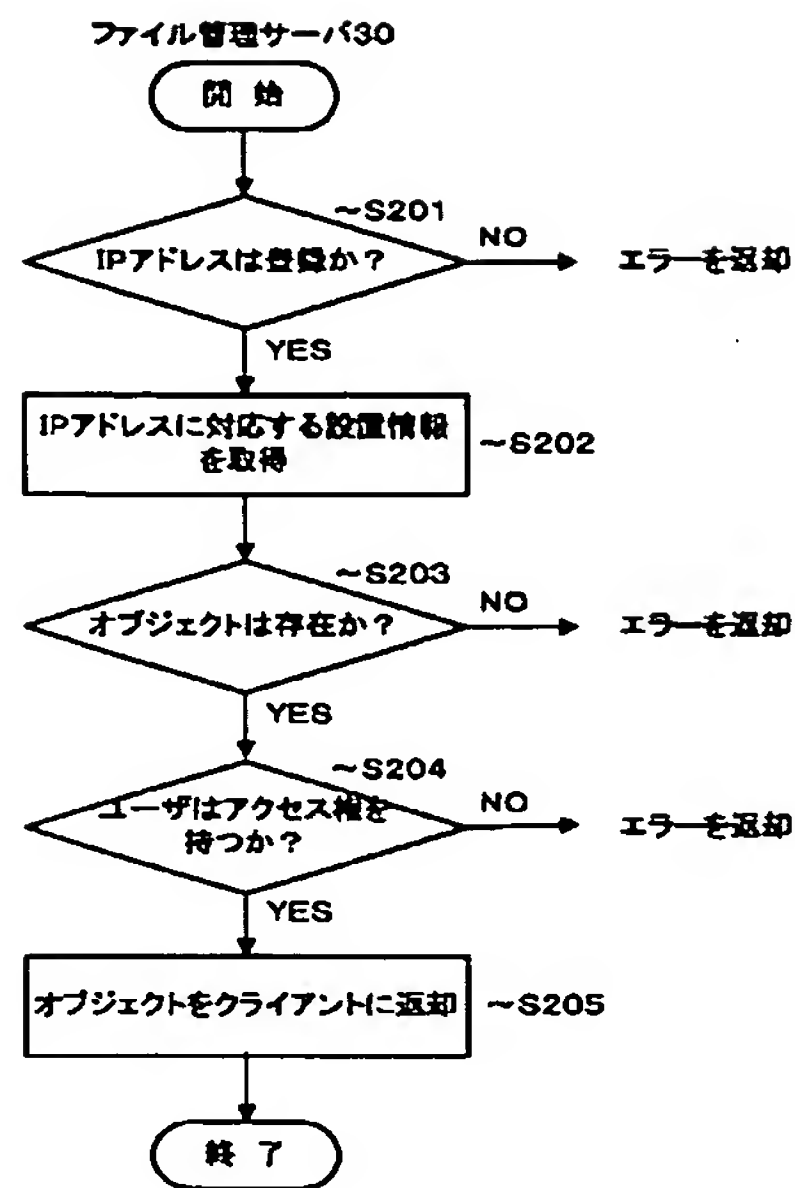
【図 5】



【図 6】



【 図 7 】



【 図 8 】

